Application of: Tobias MARTIN et al. [520.1007]
International Application No. PCT/EP00/06510
Filed Herewith

VERSION OF AMENDMENTS
WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Page1, heading before paragraph [0001]: [Specification] --Background--.

Page 1, paragraph [0001]:
[0001] The present invention relates to a method for establishing a common key within a group of subscribers [according to the definition of the species in the independent claim] using a publicly known mathematical group and a publicly known element of the group.

Page 1, paragraph [0005]:
[0005] [The] A difficulty of the DH-key exchange lies in that Alice does not know whether she actually communicates with Bob or with a cheater. In the IPSec-Standards of the Internet Engineering Task Force (IETF RFC 2412: The OAKLEY Key Determination Protocol), this problem is solved by using public key certificates in which the identity of a subscriber is combined with a public key by a trust center. In this manner, the identity of an interlocutor becomes verifiable.

Page 4, paragraph [0014]:
[0014] [The method according to] An object of the present invention [has to be suitable] is to provide a method for generating a common key within a group of at least three subscribers. The intention is for the method to be designed in such a manner that it stands out over the known methods by a small computational outlay and a small communication requirement (few rounds

even in the case of many subscribers). At the same time, however, it is intended to have a comparable security standard as the DH method. The method has to be easy to implement. Information on the structure of the group should not be required for carrying out the method.

Page 6, paragraph [0026]:

[0026] A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 or b and c are executed only by subscriber T1. In fourth method step d, all subscribers T1-Tn involved in the method compute common key k according to the [equation] assignment $k: = h(z1, g^{z2}, ..., g^{zn})$, it being required for (x1, x2, ..., xn) to be a function which is symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function g is, for instance,

$$k: = h(z1, g^{z2}, ..., g^{zn}) = g^{z1\,z1} \cdot g^{z2\,z1} \ldots g^{zn\,z1}.$$

Page 9, heading: [METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS].

Page 9 first line : --WHAT IS CLAIMED IS-- [(2) What is claimed is].

IN THE ABSTRACT:

Please amend the abstract as follows:

[The inventive method is based on] A method for establishing a common key for a group of at least three subscribers includes using a publicly known mathematical number group and a higher order element of the group $g \in G$. In the first [work] step, a message corresponding to $Ni: = g^{zi}$ mod [p)] p is sent by each subscriber to all other subscribers (Tj), (zi) being a random number chosen from the set (1, ..., p-2) by a random number generator. In the second [work] step, each subscriber (Ti) selects a transmission key $kij: = (g^{zj})^{zi}$ for each other subscriber (Tj) from the received message (g^{zj}), with $i \neq j$, for transmitting their random number (zi) to the subscribers (Tj). In the third [work] step, the common key k is calculated as k: = f(z1, z2, ..., zn) for each subscriber Ti.